Arquitectura de Seguridad Multinivel: Una Guía para las Organizaciones Modernas

Robson de Oliveira Albuquerque[1,2], Fábio Buiati[1,2], Luis Javier García Villalba[1]
[1]Grupo de Análisis, Seguridad y Sistemas (GASS), Departamento de Ingeniería del Software e Inteligencia Artificial
Facultad de Informática, Despacho 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, España
Email: {robson, fabio, javiergv}@fdi.ucm.es

[2]Faculdade de Tecnologia, Universidade de Brasília (UnB)
Curso de Engenharia de Redes de Comunicação, Departamento de Engenharia Elétrica
CEP: 70910-900 - Brasília -DF - Brasil
Email: {robson, fabio.buiati}@redes.unb.br

***Resumen*—La información puede considerarse como el activo más importante de cualquier organización moderna. Garantizar la seguridad de esta información implica preservar la confidencialidad, la integridad y la disponibilidad de la misma, tríada conocida como CIA en inglés. Este trabajo presenta una arquitectura de seguridad multinivel motivado por la necesidad de considerar la información desde diferentes puntos de vista con el fin de protegerla. Además, se sugiere una nueva clasificación de los elementos de información, operaciones, entidades y componentes que se pueden integrar para mostrar las distintas fuentes de riesgos al tratar con información sensible. Se muestra también una visión general de cómo se trata y se representa actualmente la información y por qué es tan difícil garantizar la seguridad en todos los aspectos del tratamiento de la información.**

Palabras clave*—Arquitectura, confianza, seguridad de la información.** ***(Architecture, trust, information security)

I. Introducción

La gestión de seguridad de la información es fundamental en cualquier organización. Aun así, son muy pocos los modelos formales que ayudan a proteger eficazmente la información. Una manera de tratar el problema de la seguridad de la información es gestionar los riesgos desde diferentes puntos de vista. Estos riesgos están asociados a fenómenos naturales, riesgos tecnológicos y riesgos humanos [4]. Teniendo en cuenta estos aspectos, este trabajo propone una arquitectura multinivel para la gestión de riesgos de seguridad en las organizaciones modernas. Este trabajo está organizado en 7 secciones, siendo la primera la presente introducción. La Sección II recoge los trabajos relacionados más representativos. La Sección III propone una arquitectura de seguridad multinivel. La Sección IV presenta un modelo de confianza para la arquitectura multinivel. Por último, la Sección V muestra las principales conclusiones que se extraen de este trabajo.

II. Trabajo Relacionado

Mucho se ha dicho sobre normativas y estándares en seguridad de la información y sobre la importancia de su uso. Las normas de seguridad sirven como una guía para el desarrollo de un sistema de gestión de seguridad de la información.

Normas como la BS7799 e ISO 27000 [5] son guías ampliamente reconocidas en el área de la seguridad de la información. Plataformas como ITIL y COBIT [6] son utilizadas también en la administración de las tecnologías de la información con el fin de guiar a las organizaciones a aumentar su productividad y, en algunos aspectos, ayudan a mantener la seguridad de la información en términos de organización y metodología [7].

Sin embargo, el cumplimiento de las normas no garantiza en absoluto la seguridad. Para hacer frente a la seguridad de la información se requiere ir más allá del cumplimiento de normas o de mejores prácticas.

Respecto a las arquitecturas de seguridad de la información, el Zero Trust Model for Cybersecurity [8] sostiene un mensaje muy claro: dejar de confiar en los paquetes de datos como si fuesen personas. La idea subyacente es que el concepto de redes internas y externas debe cambiarse porque uno asume que todo el tráfico no es de confianza. Zero Trust viene a decir que los datos internos deben ser protegidos contra abusos procedentes de la red interna y que los datos externos deben ser protegidos en las redes públicas.

[9] señala que existe una necesidad de mejorar la seguridad de la información a nivel administrativo y organizacional. Por su parte, [11] [10] advierten de un cambio en la manera de cómo las personan se relacionan con la seguridad de la información, convirtiéndose además en el centro del problema.

Con el fin de proteger la información, es muy importante entender la forma en que se trata en el mundo digital. Desde la perspectiva del usuario, la información puede ser un texto, una imagen o una combinación de ambos. Internet redefinió la forma de representarla y de recuperarla [12]. La representación de la información requiere de complementos estructurales o semánticas adicionales, que transforman los datos en algo significativo para los seres humanos.

Considerando todo lo expuesto anteriormente, las arquitecturas de seguridad actuales no logran gestionar los riesgos, las políticas, las personas y los activos de forma correcta. Para intentar paliar esta carencia, este trabajo propone una arquitectura de seguridad de información multinivel que trata

ISBN: 978-84-9717-323-0

de conectar todas las piezas entre sí respecto a la seguridad de la información. La especificación del modelo en niveles es importante para ver cómo todos los elementos de la arquitectura de seguridad interactúan.

III. Arquitectura de Seguridad de la Información

La forma en la que vemos la seguridad está basada en una arquitectura multinivel. En este enfoque cada elemento es una pieza del rompecabezas que debe estar bien conectada, de forma que la seguridad de información pueda ser vista como un todo indivisible. La Figura 1 ilustra la arquitectura de seguridad de la información propuesta con sus niveles.

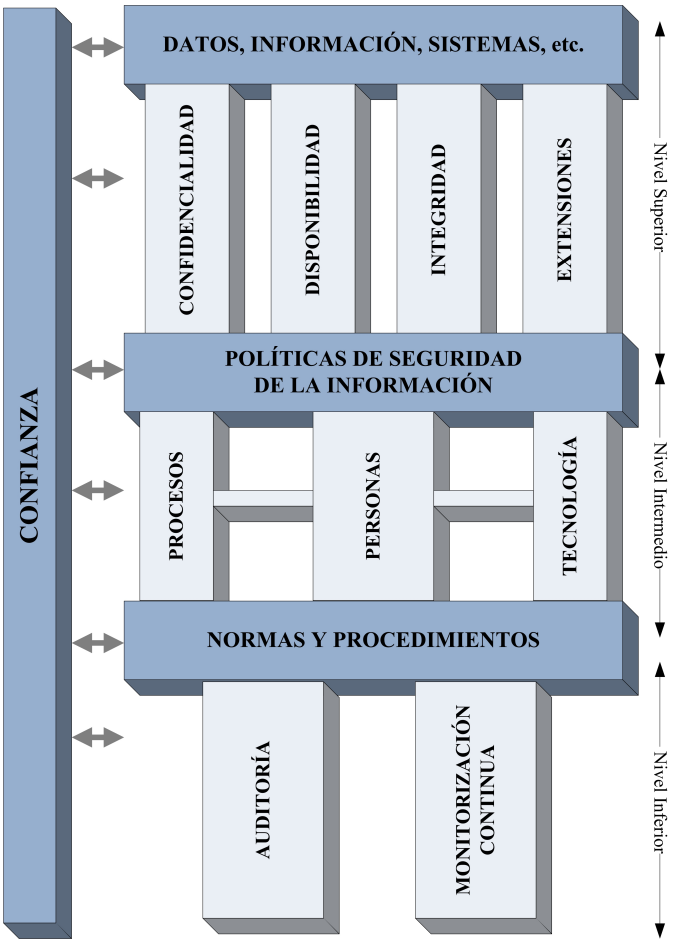

Figura 1. Arquitectura de Seguridad Multinivel

III-A. Nivel Superior

El nivel superior es la base para empezar a pensar en la seguridad de información de cualquier organización. Sin la adecuada comprensión de lo que son los datos, la información, los activos de información, etc., no hay cómo hablar de seguridad de la información, simplemente porque uno no sabe qué hay que proteger. Es importante señalar que el enfoque de "proteger todo" no es eficaz y es, además, bastante costoso.

En general, en este nivel es donde se localizan los datos importantes o con valor para las organizaciones o las personas. Considerando la importancia que tienen los datos actualmente, una gran cantidad de información se puede recuperar a partir de los datos y los sistemas de información. Utilizando herramientas y técnicas adecuadas, es posible crear además nuevos conocimientos a partir de los datos que, a simple vista, no parecen tener ningún sentido.

Cuando se trata de activos de información es muy importante que estos sean identificados y etiquetados, y la relación con la información debe ser claramente entendida por la organización.

Las redes de comunicación conectan los datos, la información y sus activos para que cualquier persona con acceso autorizado pueda explorarlas. Quién controla (personas) o cómo se controla (proceso, hardware o software) la red es lo que la hace peligrosa o no. Así que la creación de perímetros de redes, políticas y otros mecanismos de defensa sigue siendo una forma de controlar lo que entra y sale de la red. El uso de estos mecanismos es clave para entender lo que sucede en la transmisión dentro de los sistemas de información.

También en este nivel la seguridad tiene como foco salvaguardar la confidencialidad, la integridad y la disponibilidad de la información, debiendo aplicarse de forma efectiva en toda la cadena. La confidencialidad se refiere a la limitación de acceso a la información y a la divulgación a los usuarios autorizados. La integridad se refiere a la fiabilidad de los recursos de información, es decir, que los datos no han sido modificados inapropiadamente, ya sea por accidente o deliberadamente. Por último, la disponibilidad se refiere a la disponibilidad de los recursos de información.

Las extensiones de seguridad de la información son nuevos atributos o propiedades que protegen la información y los sistemas, pero no se limitan a ellos. La autenticación, el control de acceso, el no repudio, la privacidad, el anonimato y la autorización son servicios que se caracterizan como extensiones de seguridad.

III-B. Nivel Intermedio

Siguiendo un recorrido descendente nos encontramos con este nivel que es la parte de la arquitectura que nos ayudará a definir cuestiones tales quién, cómo, por qué y qué tecnologías pueden utilizarse para garantizar la seguridad de la información en el nivel superior. Los siguientes ítems son analizados: políticas de seguridad, procesos, personas y tecnología.

Una política de seguridad de la información es un documento de alto nivel que describe los requisitos o reglas que se deben cumplir para garantizar la seguridad de la información en una organización. En general, esta política es muy específica y cubre una única organización. La política de seguridad también está relacionada con los problemas de gestión y de control de la información, una vez que la protección de la misma está directamente relacionada con la cultura de la organización.

La política de seguridad debe explicar la necesidad de la seguridad de la información para todos los usuarios dentro de la organización y complementar los objetivos de la organización,

siendo necesario que esté alineada con el plan estratégico de la organización [13].

En la seguridad de la información los procesos son una manera formal de identificar, medir, gestionar y controlar los riesgos relacionados con la información o su valor para la organización. Los procesos incluyen mecanismos formales e informales (grandes o pequeños, simples o complejos, ...) para hacer las cosas y proporcionar un vínculo vital para todas las interconexiones dinámicas.

Las personas son el principal bloque del rompecabezas y representan el recurso humano. En general, una persona diseña e implementa cada parte de la política de seguridad, crea y mantiene los procesos, los activos de información, la tecnología utilizada, etc. Los problemas de seguridad afectan a las personas, sus relaciones, sus valores y sus comportamientos. Cuando se trabaja con seguridad de la información es importante hacer frente a puntos como las estrategias relacionadas con la contratación, el acceso, las responsabilidades, la formación, el despido, las sanciones y todo lo que sea importante abordar para ayudar a mantener la estrategia de seguridad de la información de la organización.

La tecnología es el elemento del rompecabezas constituido por un conjunto de sistemas de información, aplicaciones, herramientas, infraestructura y mecanismos de defensa que la organización utiliza para llevar a cabo su misión de proteger la información. Los elementos tecnológicos son susceptibles a frecuentes cambios y actualizaciones y pueden hacerse obsoletos rápidamente. La tecnología puede ser la parte fundamental de una infraestructura de la organización. La tecnología se usa también para resolver las amenazas de seguridad y los riesgos.

Es muy importante tener en cuenta que la tecnología por sí misma no hace nada. Debe ser vista como una parte de un sistema complejo que tiene necesidades específicas para proteger lo que es valioso en la organización. Además, la tecnología debe trabajar conjuntamente con personas y procesos completando un ciclo, todos ellos guiados por la política de seguridad de la información de la organización.

III-C. Nivel Inferior

Este nivel trata de las actividades diarias y las medidas que se deben adoptar en caso de un problema específico. Las prácticas de seguridad son guías para mantener la información segura. Sin embargo, las normas, procedimientos de monitorización y auditoría dan a los administradores las herramientas necesarias para ayudarles a mantener la información, los activos, las redes, los sistemas, etc., más seguros. Los siguientes ítems son analizados: normativas de seguridad, auditoría y monitorización continua.

Básicamente, una normativa define cómo deberían ser las cosas y cómo hay que valorarlas. También tiene que ver con la forma de clasificar las acciones en correctas o equivocadas. Las normativas son primordiales para la priorización de los objetivos y para definir cómo se deben hacer las cosas.

La auditoría de la seguridad de la información es un proceso que determina la valoración cualitativa y cuantitativa del estado actual del sistema analizado según criterios específicos de seguridad de la información. El proceso de auditoría es clave para encontrar riesgos, fallos técnicos, políticas, procedimientos y problemas normativos en una organización. Hay que tener en cuenta que la auditoría es un proceso que nunca termina. Cuando se realiza la auditoría, uno debe estar preparado para abarcar temas desde seguridad física de los centros de datos hasta la seguridad lógica, incluyendo los perímetros de red, la configuración del sistema y los sistemas de información.

Otra de las tareas realizadas en este nivel es la monitorización continua. Se trata de una actividad de mantenimiento de los conocimientos de seguridad de la información, vulnerabilidades, amenazas y riesgos asociados [14]. Es un punto clave de apoyo a la toma de decisiones relativas a la gestión de riesgos de una organización.

La monitorización continua se inicia definiendo qué, cómo, por qué y cuándo monitorizar los activos de información o cualquier parte de la arquitectura. Se apoya en tecnología, procesos, procedimientos, entornos operativos y personas. También ayuda en el establecimiento de prioridades y gestiona el riesgo de forma coherente en toda la organización.

IV. Confianza

Desde el punto de vista de la seguridad de la información, la confianza puede tener un valor de cero o de uno. Uno confía o no en sus sistemas de información, redes, activos, etc. El “tal vez” debe evitarse a toda costa. Por lo general, la confianza se adquiere mediante la observación empírica, por prueba formal de los sistemas, etc. [15].

La confianza y la seguridad están estrechamente relacionadas [15]. Si se consideran los objetivos de seguridad, está claro que los aspectos de confianza están conectados con la seguridad ya que mantener la información segura depende de las personas, las extensiones de seguridad (autenticación, autorización, control de acceso, no repudio, etc.).

Considerando lo anteriormente expuesto, no se puede proteger la información sin ser capaz de comprender todo el ciclo de vida que tiene la información. Hay que tener en cuenta una visión detallada si se desea más seguridad en el sistema; uno debe ser capaz de representar, procesar y utilizar la información en un entorno donde las personas, la tecnología, los activos de información, el hardware, el software, etc., están conectados entre sí. Y, paralelamente, hay que tomar medidas de seguridad para garantizar su protección. Ahí es donde la arquitectura de seguridad de la información multinivel con confianza entra en escena porque sólo proteger una parte de la información se ha demostrado ineficaz, como se ha visto recientemente [1][2].

La confianza en general es parte del rompecabezas cuando hay un conocimiento suficiente de la información, los sistemas, la tecnología y los demás componentes que ayudan hacer afirmaciones como “totalmente seguro” o la información es segura porque se cumple alguna condición en particular. Esta arquitectura en niveles le permite a uno hacer frente a determinados componentes y aislar problemas relacionados con cada uno de ellos.

V. Conclusiones

La tarea de garantizar la seguridad de la información no es un fin en sí mismo; es un medio para lograr un fin [16]. Se trata también de un tema en constante evolución, debido a la creciente magnitud y complejidad de las amenazas de seguridad de la era digital. Como se observa en la actualidad, el campo de investigación de la seguridad de información es cada vez más importante porque el mundo está interconectado con redes de comunicación que se utilizan para la transmisión de información crítica y sensible.

En este trabajo se ha introducido una arquitectura de seguridad multinivel donde los elementos de seguridad de la información están interconectados siendo útiles para la gestión de riesgos en los diferentes niveles de la organización. De esta forma, la seguridad de la información puede ser vista como un todo.

Gobierno, organizaciones y empresas que consideran la gestión de seguridad de la información necesitan un enfoque sistemático para abordar de manera coherente la seguridad en cada nivel, disminuyendo así los riesgos de administración y mejorando la eficiencia de la gestión de la seguridad. Bajo esta perspectiva, la arquitectura de seguridad de la información en niveles puede ser utilizada como una guía para obtener mejores resultados en la protección de la información.

Agradecimientos

Los autores también agradecen el apoyo proporcionado por el Laboratorio de Tecnologías de Decisión de la Universidad de Brasilia (LATITUDE / UnB). Asimismo, Fábio quiere agradecer la financiación que le brinda el Programa Nacional de Post-Doctorado de Brasil (PNPD/CAPES). El Grupo de Investigación GASS agradece la infraestructura proporcionada por el Campus de Excelencia Internacional (CEI) Campus Moncloa - Clúster de Cambio Global y Nuevas Energías (y, más concretamente, el sistema EOLO como recurso de computación de alto rendimiento HPC - High Performance Computing), infraestructura financiada por el Ministerio de Educación, Cultura y Deporte (MECD) y por el Ministerio de Economía y Competitividad (MINECO).

Referencias

[1] G. Greenwald, E. MacAskill, L. Poitras, “Edward Snowden: the whistleblower behind the NSA surveillance revelations,” *The Guardian*, Vol. 9, 2013.

[2] J.-T. Richelson, “The Snowden Affair. Web Resource Documents the Latest Firestorm over the National Security Agency,” *National Security Archive Electronic Briefing Book*, No. 436, 2013.

[3] Gartner Press Release. “Gartner Says Cloud-Based Security Services Market to Reach 2.1 Billion dollars in 2013”, Stamford, Conn., 2013. Disponible en ttp://www.gartner.com/newsroom/id/2616115.

[4] B. Blakley, E. McDermott, D. Geer, “Information security is information risk management,” *ACM Proceedings of the Workshop on New security Paradigms*, pp. 97–104, 2001.

[5] M. Whitman, H. Mattord, “Management of Information Security,” *Cengage Learning, Fourth Edition*, 2013.

[6] R. Parvizi, F. Oghbaei, S. R. Khayami, “Using COBIT and ITIL frameworks to establish the alignment of business and IT organizations as one of the critical success factors in ERP implementation,” *5th Conference on Information and Knowledge Technology (IKT)*, 2013 pp. 274–278, 2013.

[7] Department of Communications, Information Technology and the Arts and the Trusted Information Sharing Network. “Secure Your Information: Information Security Principles for Enterprise Architecture,” *Report, Australia*, 2007.

[8] The National Institute of Science and Technology (NIST), “Developing a Framework to Improve Critical Infrastructure Cybersecurity. Submitted by Forrester Research. In Response to RFI# 130208119-3119-01”, 2013. Disponible en http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf.

[9] R.-M. Ahlfeldt, P. Spagnoletti, G. Sindre. “Improving the Information Security Model by using TFI”, *In the New Approaches for Security, Privacy and Trust in Complex Environments. IFIP International Federation for Information Processing*, Vol. 232, pp. 73–84, 2007.

[10] R. Blakley, A. Johnston, P. Lowry, Q. Hu, M. Warkentin, R. Baskerville, “Future directions for behavioral information security research,” *Computers & Security*, Volume 32, February 2013, pp. 90–101.

[11] S. Aurigemma, R. Panko, “A Composite Framework for Behavioral Compliance with Information Security Policies”, *In proceedings of the 45th Hawaii International Conference on System Sciences. IEEE Computer Society*, 2012.

[12] H. Chu, “Information Representation and Retrieval in the Digital Age”, *Information Today, Inc*, Second Edition, 2010.

[13] ISACA. “An Introduction to the Business Model for Information Security”, 2009, Disponible en http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf.

[14] The National Institute of Science and Technology (NIST), “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”, *NIST Special Publication*, pp. 800–137, 2011.

[15] P. Lamsal, “Understanding Trust and Security”, *Department of Computer Science. University of Helsinki, Finland*, 2001.

[16] T. Peltier, “Information security fundamentals,” *CRC Press*, 2013.